Mumbai University Question Paper

B.Sc.IT: Semester - V

Network Security

November - 2017 | 75:25 Pattern

Time: 2 ½ Hours **Total Marks:** 75

N.B.: **(1)** *All Question are Compulsory.*
(2) *Make Suitable Assumptions Wherever Necessary And State The Assumptions Made.*
(3) *Answer To The Same Question Must Be Written Together.*
(4) *Number To The Right Indicates Marks.*
(5) *Draw Neat Labeled Diagrams Wherever Necessary.*
(6) *Use of Non – Programmable Calculator is allowed.*

Q.1 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) Explain different principles of security. **(5)**
(B) List and explain different types of Criminal Attacks. Give example of each one. **(5)**
(C) List different Transposition Techniques. Explain any one with example. **(5)**
(D) A and B want to establish a secrete key using the Diffie-Hellman Kay Exchange protocol. Assuming the values as n=11,g=5,x=2 and y=3, find out the values of A,B and the secret key. **(5)**

Q.2 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) Explain Cipher Feedback Mode. **(5)**
(B) Explain DES Algorithm. **(5)**
(C) How subkey is generated for rounds of IDEA Algorithm? **(5)**
(D) Explain the working of RC5. **(5)**

Q.3 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) Explain with example RSA algorithm. **(5)**
(B) Write down difference between Symmetric and Asymmetric Key Cryptography. **(5)**
(C) Explain how MD5 works. **(5)**
(D) What is Message Authentication Code? Write down disadvantages of Hash-Based Message Authentication Code. **(5)**

Q.4 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) List and explain various fields in a X.509 Digital Certificate Version 3. **(5)**
(B) What is need of Self-Signed Digital Certificates and cross certificate? **(5)**
(C) Write down the difference between online certificate revocation status checks and simple certificate validation protocol. **(5)**
(D) List and explain PKIX Services. **(5)**

Q.5 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) Explain the Purchase Request Transaction of SET. **(5)**
(B) List different Email Security Protocols. Explain any one in detail. **(5)**
(C) Explain IP Datagram Format. **(5)**
(D) List and explain different Fields of Security Association Database. **(5)**

Q.6 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) What is Authentication Token? **(5)**
(B) What is the use of Smart Cards? Write down the problems and their solutions related to Smart Card Technology. **(5)**
(C) Write a short note on Kerberos. **(5)**
(D) Write a short note on One Way Authentication. **(5)**

[TURN OVER]

Q.7 ATTEMPT ANY THREE QUESTIONS: (15 MARKS)

(A) List and explain different types of Attacks. **(5)**

(B) Explain how subkey is generated in Blowfish Algorithm. **(5)**

(C) Write down difference between MD5 and SHA-1. **(5)**

(D) List different Public Key Cryptography Standards. Explain any two of them. **(5)**

(E) What is Electronic Money? Classify Electronic Money based on **(5)**

(i) *Tracking of money*

(ii) *Involvement of the bank in the transaction*

(F) List and explain different approaches to achieve SSO. **(5)**